IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AMELIA INGRAO AND ELISABETH PACANA, Plaintiffs, v. ADDSHOPPERS, INC., NUTRISYSTEM, INC., AND VIVINT, INC., Defendant.	CIVIL ACTION NO. 24-1022

OPINION

Slomsky, J. **November 25, 2024**

TABLE OF CONTENTS

I. INTRODUCTION

This case arises out of Defendant AddShoppers, Inc.'s ("Defendant AddShoppers" or "AddShoppers") alleged surreptitious tracking of Plaintiff Amelia Ingrao's ("Plaintiff Ingrao" or "Ingrao") and Plaintiff Elisabeth Pacana's ("Plaintiff Pacana" or "Pacana") (collectively "Plaintiffs") internet browsing activity. (See Doc. No. 1.) Plaintiffs allege Defendant AddShoppers, through its partnerships with retailers such as Defendant Nutrisystem, Inc. ("Defendant Nutrisystem" or "Nutrisystem") and Defendant Vivint, Inc. ("Defendant Vivint" or "Vivint"), impermissibly tracked Plaintiffs' internet browsing activity and compiled their personal information into consumer profiles. (Id. at ¶¶ 36-37.) Through these profiles, AddShoppers allegedly linked Plaintiffs' online browsing activity with their personal information, such as their email addresses, in order to send Plaintiffs targeted ads based on their browsing activity. (Id.)

Plaintiffs filed a Complaint against Defendant AddShoppers, Defendant Nutrisystem, and Defendant Vivint (collectively "Defendants"), alleging claims under the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA") (Counts I, II, and III), the California Invasion of Privacy Act ("CIPA") (Count IV) and California's Computer Access and Data Fraud Act ("CDAFA") (Count V). (Id. at ¶¶ 81-148.)

Specifically, in Count I, Plaintiff Ingrao alleges a WESCA claim against Defendant Nutrisystem. (Id. at ¶¶ 81-95.) Similarly, Plaintiff Pacana brings WESCA claims against Defendant AddShoppers and Defendant Vivint in Counts II and III, respectively. (Id. at ¶¶ 96-125.) In Count IV, Plaintiff Ingrao alleges a CIPA claim against Defendant Nutrisystem. (Id. at ¶¶ 126-34.) Finally, in Count V, Plaintiff Ingrao brings a CDAFA claim against Defendants AddShoppers and Nutrisystem. (Id. at ¶¶ 135-48.) In response, Defendants each filed Motions to Dismiss the Complaint. (Doc. Nos. 25, 26, 31.)

Defendant Vivint argues dismissal is proper under Federal Rule of Civil Procedure 12(b)(1) because Plaintiffs lack Article III standing. (Doc. No. 26 at 11-14.) Defendant AddShoppers submits dismissal is warranted under Federal Rule of Civil Procedure 12(b)(2) because the Court lacks personal jurisdiction over it. (Doc. No. 31-1 at 11-17.) And each of the three Defendants argues for dismissal because Plaintiffs fail to state a claim under Federal Rule of Civil Procedure 12(b)(6). (See generally Doc. Nos. 25, 26, 31.)

As explained more thoroughly below, Defendants' Motions to Dismiss (Doc. Nos. 25, 26, 31) will be granted for the following reasons.[1] First, Plaintiffs fail to allege sufficient harm to establish Article III standing. Plaintiffs argue Defendants' action of collecting their internet browsing activity and personal email addresses is sufficient to establish harm because it is analogous to the capture of sensitive personal information protected by common law privacy torts. (Doc. No. 39 at 15; Doc. No. 69 at 7-8.) But this Court joins other courts, including courts in the Third Circuit, that have held that a person's internet browsing activity and email address is not sufficiently sensitive information to support the concrete injury requirement for Article III standing.[2] Second, the Court does not have personal jurisdiction over Defendant AddShoppers

[1] In its Motion to Dismiss, Defendant Nutrisystem requested that, as an alternative to dismissing the Complaint, "the Court should strike the class claims brought by Ingrao against Nutrisystem, and stay the litigation of her individual claims pending the outcome of a further-advanced California lawsuit," McClung v. AddShoppers, Inc., No. 23-cv-01996. (See Doc. No. 25 at 20-26.) Defendant AddShoppers similarly argues that if any of Plaintiffs' claims survive the Motions to Dismiss, the case should be "stayed pending the outcome of the putative class action matter pending in the Northern District of California, styled as McClung v. AddShoppers, Inc. et al." (Doc. No. 31 at 2.) Because the Court will grant Defendants' Motions to Dismiss in their entirety, it need not consider Nutrisystem's request to strike nor Nutrisystem and AddShoppers' request to stay the case.

[2] Courts to consider this issue have concluded as follows: In re BPS Direct, LLC, 705 F. Supp. 3d 333, 353 (E.D. Pa. 2023) (holding "browsing activity is not sufficiently private to establish concrete harm" as needed for Article III standing); Cook v. GameStop, 689 F. Supp. 3d 58, 66 (W.D. Pa. 2023) (concluding that the plaintiff's internet browsing activity was not sufficiently

because AddShoppers' actions satisfy neither the Calder "effects" test nor the traditional test for specific jurisdiction. Finally, because Plaintiffs fail to plead both that Defendants intercepted their communications in Pennsylvania, and that Defendants intercepted the contents of their communications, they fail to state a claim under the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA") and the California Invasion of Privacy Act ("CIPA"). Similarly, because Plaintiff Ingrao fails to allege she suffered the requisite damage or loss, she fails to state a claim under the California Computer Access and Data Fraud Act ("CDAFA").

II. BACKGROUND

A. Parties

The named Plaintiffs in this Class Action Complaint are Plaintiff Amelia Ingrao and Plaintiff Elisabeth Pacana. (See Doc. No. 1 at 1.) Plaintiff Ingrao is a resident and domiciliary of California. (Id. at ¶ 6.) Plaintiff Pacana is a resident and domiciliary of Pennsylvania. (Id. at ¶ 7.)

Defendant AddShoppers is a Delaware corporation with its principal place of business in North Carolina. (Id. at ¶ 8.) Defendant Nutrisystem is a Pennsylvania corporation with its principal place of business in Pennsylvania. (Id. at ¶ 9.) Defendant Vivint is a Delaware corporation with its principal place of business in Utah. (Id. at ¶ 10.)

---

private information to support Article III standing); Farst v. Autozone, Inc., 700 F. Supp. 3d 222, 230 (M.D. Pa. 2023) (holding the plaintiff had failed to establish Article III standing because the defendant's capture of information such as his "keystrokes, mouse clicks, and search history while he surfed [the defendant's] website" was not private information); I.C. v. Zynga, Inc., 600 F. Supp. 3d 1034, 1049-50 (N.D. Cal. 2022) (holding "basic contact information, including one's email address" is not sensitive personal information to support Article III standing); Brignola v. Home Properties, L.P., No. 10-3884, 2013 WL 1795336, at *12 (E.D. Pa. Apr. 26, 2013) (holding information including the plaintiff's name, address, and phone number was not private information).

B. Factual Background

1. Defendant AddShoppers' "SafeOpt" Program

Defendant AddShoppers is alleged to run a marketing program called "SafeOpt" that tracks individuals' internet browsing activity, collects their personal information gleaned from their browsing activity, such as their email addresses, and then uses this information to send them targeted advertisements.[3] (Id. at ¶¶ 2, 3.) SafeOpt is available to both consumers and businesses. (Id. at ¶ 3.) For consumers, SafeOpt is marketed as a service they "can voluntarily opt into to 'receive verified offers from SafeOpt's brand partners.'" (Id.) For businesses, SafeOpt is marketed as an "opportunity to 'send 3-5x more emails to shoppers who abandon your website' by 'using our list of 175M+ U.S. shoppers.'" (Id. at ¶ 21.) When a business opts into SafeOpt, it becomes a partner in AddShoppers' "Data Co-Op," meaning AddShoppers through SafeOpt is granted access to the business's User Data. (Id. at ¶¶ 27-28.) User Data "collects and pools the sensitive personal information provided by individuals to online retailers in confidence, creates dossiers on those individuals, and then tracks them across the internet to monitor their web browsing" activity. (Id. at ¶ 29.) Defendant Nutrisystem and Defendant Vivint are alleged to be partners with AddShoppers and members of its Data Co-Op. (See id. at ¶¶ 55-56, 66.)

SafeOpt collects its partners' User Data and tracks consumers' internet browsing activity through third-party tracking cookies. (Id. at ¶ 33.) "Cookies are small text files that are stored on a user's computer or mobile device by a website. They are used to save information about the user's browsing activity, such as login information, shopping cart contents, and browsing history." (Id.) In contrast to a first-party cookie which is created and stored by the website the user is visiting

[3] As described below, the personal information AddShoppers allegedly collects through SafeOpt is the individual's internet browsing history, such as data on the dates and times they visit certain websites, as well as their email addresses. (See Doc. No. 1 at ¶¶ 56-57, 62-63, 66.)

(also called the host domain), a third-party cookie is created by a different domain than the host domain. (Id. at ¶¶ 34-35.) "These cookies are accessible on any website that loads the third-party server's code. Because they can be accessed by multiple domains, third-party cookies can be used to track a user's browsing activity across multiple websites." (Id.)

When a business partners with AddShoppers and joins its Data Co-Op, that business agrees to install AddShoppers' third-party tracking cookie code on its website. (Id. at ¶ 36.) According to Plaintiffs, this code allows AddShoppers to surreptitiously track consumers' internet activity to send them targeted advertisements using the following method:

> When an internet user creates an account or makes a purchase with the business, a third-party tracking cookie is created that includes a unique value AddShoppers associates with that user. The cookie is hidden on the user's browser and automatically sends information to AddShoppers' SafeOpt domain . . . AddShoppers then associates that unique value with the personal information the user provided to the company, which typically includes, at a minimum, full name, address, payment card information, and email address.
>
> With the tracking cookie hidden in the user's browser, AddShoppers can monitor the user's browsing activity across the internet. If the user lands on another website in the SafeOpt network, the cookie values "sync" and AddShoppers tracks the user's activity on the website, including the user's detailed referrer Uniform Resource Locator ("URL"). Because AddShoppers already associates personal information with the cookie value, it can directly advertise to the user even where the user leaves a website without affirmatively providing any personal information.

(Id. at ¶¶ 36-37.) AddShoppers typically sends these direct advertisements to consumers "in the form of a direct email from the retailer 'via SafeOpt' imploring the user to return to the [retailer's] website to purchase a product they were looking at." (Id. at ¶ 41.) AddShoppers then keeps a portion of the profit from sales made "via affiliate links in emails, texts, apps, and content." (Id.)

2. Plaintiff Amelia Ingrao's Allegations

Plaintiff Ingrao alleges that she visited Defendant Nutrisystem's website for the first time on January 27, 2024. (Id. at ¶ 55.) She further alleges that Defendant AddShoppers, through SafeOpt, tracked her precise website visit because, despite never providing any personal

information to Nutrisystem, Ingrao received an email to her personal email account from "Nutrisystem via SafeOpt" later that same evening. (Id. at ¶¶ 56-57.) Prior to this occurring, Ingrao had never heard of SafeOpt. (Id. at ¶ 59.) After she received the email, Plaintiff Ingrao "requested her data from AddShoppers and discovered she had been tracked by many companies for several years." (Id.)

3. Plaintiff Elisabeth Pacana's Allegations

Plaintiff Pacana alleges that she visited "the website of a retailer called Lamin-x" on February 22, 2024.[4] (Id. at ¶ 61.) She further alleges that Defendant AddShoppers, through SafeOpt, tracked her precise website visit because, despite never providing any personal information to Lamin-x, she later received an email to her personal email account from "Lamin-x via SafOpt." (Id. at ¶¶ 62-63.) Prior to receiving this email, Pacana had never heard of SafeOpt. (Id. at ¶ 65.) After she received the email, she "requested her data from AddShoppers and discovered she had been tracked by at least a dozen companies for several years, including the exact dates and times she visited other websites that (unbeknownst to her) were part of the AddShoppers network." (Id. at ¶ 66.) One of these websites that had tracked her was Defendant Vivint, "which surreptitiously captured information about Plaintiff Pacana's visit to its website on January 24, 2023." (Id.)

C. Procedural Background

On March 8, 2024, Plaintiffs filed their Complaint. (Doc. No. 1.) On May 6, 2024, Defendant Nutrisystem filed a Motion to Dismiss the Complaint. (Doc. No. 25.) On May 10, 2024, Defendant Vivint and Defendant AddShoppers each filed a Motion to Dismiss the Complaint. (Doc. Nos. 26, 31.) On June 7, 2024, Plaintiffs filed a Memorandum in Opposition to

[4] Plaintiff Pacana did not include Lamin-x as a defendant in this lawsuit.

Defendants' Motions to Dismiss. (Doc. No. 39.) On July 26, 2024, Defendants each filed a Reply in Support of their Motions to Dismiss. (Doc. Nos. 53, 55, 56.) On September 13, 2024, the Court held a hearing on the Motions. (See Doc. No. 62.) On October 15, 2024, the parties each filed a Supplemental Memorandum in support of their respective positions regarding the Motions. (Doc. Nos. 66, 67, 68, 69.) The Motions are now ripe for disposition.

III. STANDARD OF REVIEW

A. Standard on a Motion to Dismiss for Lack of Standing Under Federal Rule of Civil Procedure 12(b)(1)

A motion to dismiss for lack of standing is brought under Federal Rule of Civil Procedure 12(b)(1) because standing is a jurisdictional matter. Const. Party of Pa. v. Aichele, 757 F.3d 347, 357 (3d Cir. 2014) (internal citation omitted). A district court considering a motion pursuant to Rule 12(b)(1) must first determine whether that motion presents a "facial" attack or a "factual" attack on the claim at issue "because that distinction determines how the pleading must be reviewed." Id. A facial challenge contests the sufficiency of the complaint because of a defect on its face, such as lack of diversity among the parties or the absence of a federal question. See Mortensen v. First Fed. Sav. & Loan Ass'n, 549 F.2d 884, 891 (3d Cir. 1977). In a facial challenge, the court must consider the allegations of the complaint as true and consider only those allegations in the complaint and the attached documents in deciding whether the plaintiff has sufficiently alleged a basis for subject-matter jurisdiction. See Gould Elecs. Inc. v. United States, 220 F.3d 169, 176 (3d Cir. 2000); see also U.S. ex rel. Atkinson v. Pa. Shipbuilding Co., 473 F.3d 506, 514 (3d Cir. 2007) (terming a facial attack as "an alleged pleading deficiency"). Thus, a court applies the same standard of review used in considering a motion to dismiss under Rule 12(b)(6).

A factual attack, on the other hand, challenges the actual failure of the plaintiff's claims to "comport with the jurisdictional prerequisites." Pa. Shipbuilding, 473 F.3d at 514. Such an

evaluation may occur at any stage of the proceeding, but only after the defendant has filed an answer. Mortensen, 549 F.2d at 891-92. When a court is confronted with a factual attack, "[it] is free to weigh the evidence and satisfy itself as to the existence of its power to hear the case," and the plaintiff bears the burden of showing that jurisdiction does in fact exist. Id. A district court may consider evidence outside the pleadings. Gould Elecs. Inc., 220 F.3d at 176 (internal citation omitted). No presumption of truthfulness attaches to the plaintiff's allegations, such that the existence of disputed material facts does not preclude a court from evaluating the merits of jurisdictional claims. Mortensen, 549 F.2d at 891.

B. Standard on a Motion to Dismiss for Lack of Personal Jurisdiction Pursuant to Federal Rule of Civil Procedure 12(b)(2)

Federal Rule of Civil Procedure 12(b)(2) provides that a motion to dismiss may be filed when the court does not have personal jurisdiction over a defendant. "Once challenged, the plaintiff bears the burden of establishing personal jurisdiction." O'Connor v. Sandy Lane Hotel Co., 496 F.3d 312, 316 (3d Cir. 2007) (citation omitted). To show personal jurisdiction, the plaintiff may rely on the allegations in the complaint, affidavits, or other evidence. Metcalfe v. Renaissance Marine, Inc., 566 F.3d 324, 330 (3d Cir. 2009) (internal quotation and citation omitted). However, to "survive a Rule 12(b)(2) motion to dismiss, a plaintiff may not merely rely on the allegations in its complaint." Deardorff v. Cellular Sales of Knoxville, Inc., Civil Action No. 19-2642-KSM, 2020 WL 5017522, **1-2 (E.D. Pa. Aug. 25, 2020) (emphasis in the original) (citation omitted). If the court "does not conduct [an] evidentiary hearing . . . [the] plaintiff need only plead [a] prima facie case" of jurisdiction to defeat a motion to dismiss. Carteret Sav. Bank v. Shushan, 954 F.2d 141, 142 n.1 (3d Cir. 1992) (citations omitted). In deciding a motion to dismiss for lack of personal jurisdiction, the court "must accept all of the plaintiff's allegations as true and construe disputed facts in favor of the plaintiff." Id. (citations omitted).

C. Standard on a Motion to Dismiss Pursuant to Federal Rule of Civil Procedure (12)(b)(6)

The motion to dismiss standard under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted is set forth in Ashcroft v. Iqbal, 556 U.S. 662 (2009). After Iqbal, it is clear that "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice" to defeat a Rule 12(b)(6) motion to dismiss. Id. at 678; see also Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007). "To survive dismissal, 'a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.'" Tatis v. Allied Interstate, LLC, 882 F.3d 422, 426 (3d Cir. 2018) (quoting Iqbal, 556 U.S. at 678). Facial plausibility is "more than a sheer possibility that a defendant has acted unlawfully." Id. (quotation marks omitted) (quoting Iqbal, 556 U.S. at 678). Instead, "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. (quotation marks omitted) (quoting Iqbal, 556 U.S. at 678). In assessing the plausibility of a claim, the court must "accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief." Fowler v. UPMC Shadyside, 578 F.3d 203, 210 (3d Cir. 2009).

Applying the principles of Iqbal and Twombly, the Third Circuit Court of Appeals in Santiago v. Warminster Township, 629 F.3d 121 (3d Cir. 2010), set forth a three-part analysis that a district court in this Circuit must conduct in evaluating whether allegations in a complaint survive a Rule 12(b)(6) motion to dismiss:

> First, the court must "tak[e] note of the elements a plaintiff must plead to state a claim." Second, the court should identify allegations that, "because they are no more than conclusions, are not entitled to the assumption of truth." Finally, "where

> there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement for relief."

Id. at 130 (alteration in original) (quoting Iqbal, 556 U.S. at 675, 679). The inquiry is normally broken into three parts: "(1) identifying the elements of the claim, (2) reviewing the complaint to strike conclusory allegations, and then (3) looking at the well-pleaded components of the complaint and evaluating whether all of the elements identified in part one of the inquiry are sufficiently alleged." Malleus v. George, 641 F.3d 560, 563 (3d Cir. 2011).

A complaint must do more than allege a plaintiff's entitlement to relief, it must "show" such an entitlement with its facts. Fowler v. UPMC Shadyside, 578 F.3d 203, 210-11 (3d Cir. 2009) (citing Phillips v. Cnty. of Allegheny, 515 F.3d 224, 234-35 (3d Cir. 2008)). "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'show[n]'—'that the pleader is entitled to relief.'" Iqbal, 556 U.S. at 679 (second alteration in original) (citation omitted). The "plausibility" determination is a "context-specific task that requires the reviewing court to draw on its judicial experience and common sense." Id.

IV. ANALYSIS

A. Plaintiffs Lack Article III Standing to Bring Their Claims Against Defendants

Because Plaintiffs fail to allege they suffered a concrete harm, they lack Article III standing to bring their respective claims against Defendants. While only Defendant Vivint raised the issue of standing in a facial attack on Plaintiff Pacana's claim against Vivint, the Court will also consider Plaintiffs' standing to bring claims against Defendant AddShoppers and Defendant Nutrisystem.[5]

[5] Defendant Vivint's challenge under Federal Rule of Civil Procedure 12(b)(1) is a facial challenge, rather than a factual challenge, to Plaintiff Pacana's claim against Defendant Vivint because the challenge does "not dispute what [the] facts are, but rather whether the facts as

See Meyer v. Delaware Valley Lift Truck, Inc., 392 F. Supp. 3d 483, 494 (E.D. Pa. 2019) ("[S]tanding is jurisdictional and thus may be raised sua sponte . . . .") (citing Frissell v. Rizzo, 597 F.2d 840, 843 (3d Cir. 1979)).

Under Article III of the United States Constitution, the power of the judiciary extends only to "cases" and "controversies." Spokeo, Inc. v. Robins, 578 U.S. 330, 337 (2016). An element of the case-or-controversy requirement is that a plaintiff must establish, based on their complaint, that they have standing to bring the case. Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 110 (3d Cir. 2019). To establish standing, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." TransUnion LLC v. Ramirez, 594 U.S. 413, 423 (2021).

For a harm to be "particularized, . . . it must affect the plaintiff in a personal and individual way." Spokeo, 578 U.S. at 339. For a harm to be "concrete," the "injury must be 'de facto'; that is, it must actually exist." Id. at 340 (citing Black's Law Dictionary 479 (9th ed. 2009)). "Central to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts." TransUnion, 594 U.S. at 417. "That inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury." Id. at 425. In other words, a court must determine whether "the kind of harm a plaintiff alleges" is closely related to "the kind of harm caused by the

ple[d] create standing." Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 110 (3d Cir. 2019). Accordingly, the Court will consider the allegations in the Complaint as true and will only consider these allegations in deciding whether Plaintiffs have sufficiently alleged a basis for subject-matter jurisdiction. See Gould Elecs. Inc. v. United States, 220 F.3d 169, 176 (3d Cir. 2000) (holding a court should apply the same standard of review on a Rule 12(b)(1) motion raising a facial challenge as the standard applied on a Rule 12(b)(6) motion).

comparator tort." Barclift v. Keystone Credit Services, LLC, 93 F.4th 136, 144-45 (3d Cir. 2024). However, merely alleging a "bare procedural violation, divorced from any concrete harm," is insufficient to establish Article III standing. Kamal, 918 F.3d at 111 (quoting Spokeo, 578 U.S. at 341).

Here, Plaintiffs' asserted harm is Defendant AddShoppers' aggregation of Plaintiffs' internet browsing activities, specifically the dates and times they visit AddShoppers' partner websites, along with their email addresses. (Doc. No. 69 at 4-5.) And because AddShoppers cannot aggregate Plaintiffs' internet browsing activity and email addresses without the knowing participation of retailers like Nutrisystem and Vivint, Plaintiffs argue that Defendants Nutrisystem and Vivint have contributed to the asserted harm. (Doc. No. 39 at 16.) In analogizing this harm to one traditionally recognized as providing a basis for a lawsuit in American courts, Plaintiffs contend the asserted harm bares a "close relationship" to an "intrusion on privacy and seclusion that can be vindicated in federal courts," including the common law torts of public disclosure of private information and the right to privacy regarding personal information. (Doc. No. 39 at 15; Doc. No. 69 at 7-8.)

But these common law privacy torts necessarily require the information disclosed to be private or personal information. For example, the Third Circuit characterized the harm caused by the tort of public disclosure of private information as "the humiliation that accompanies the disclosure of sensitive or scandalizing private information to public scrutiny." Barclift, 93 F.4th at 145-56 (emphasis added). Similarly, courts have recognized that the harm caused by the intrusion upon seclusion involves the disclosure of private and personal information. See In re BPS Direct, LLC, 705 F. Supp. 3d 333, 351 (E.D. Pa. 2023) ("[The plaintiffs] analogize their harms to intrusion upon seclusion and public disclosure of private facts– torts which require the

interception or disclosure of private and personal information. The protections which existed traditionally at common law existed only as to private information.") (emphasis in original); Cook v. GameStop, Inc., 689 F. Supp. 3d 58, 65 (W.D. Pa. 2023) ("The requirement of private facts or private affairs in both [the public disclosure of private information and intrusion upon seclusion] torts confirms that the nature of the information is paramount.") Based on these characterizations of the harms protected by the common law privacy torts, to establish a "close relationship" between the asserted harm and one traditionally recognized as providing a basis for a lawsuit, Plaintiffs must allege the disclosure of their private or personal information.

But here, the only information of Plaintiffs that Defendants are alleged to have collected are their internet browsing activities and email addresses. (See Doc. No. 1 at ¶¶ 56-57, 62-63, 66.) And neither internet browsing activity nor email addresses qualify as private or personal information. See BPS Direct, 705 F. Supp. 3d at 353 ("[B]rowsing activity is not sufficiently private to establish concrete harm."); Cook v. GameStop, Inc., 689 F. Supp. 3d at 66 (holding the plaintiff's internet browsing activity was not personal information to support Article III standing because, at most, internet browsing information relates to product preferences and "[p]roduct preference information is not personal information"); I.C. v. Zynga, Inc., 600 F. Supp. 3d 1034, 1049-50 (N.D. Cal. 2022) (holding the disclosure of "basic contact information, including one's email address" is inadequate to establish Article III standing based on the "insufficient fit between the loss of information alleged here and the common law privacy torts of . . . disclosure of private facts and intrusion upon seclusion"); see also Brignola v. Home Properties, L.P., No. 10-3884, 2013 WL 1795336, at *12 (E.D. Pa. Apr. 26, 2013) ("The information alleged to be reported (and included in the exhibits) are Plaintiff's name, address, phone number, etc. These are not private facts actionable for an intrusion upon seclusion claim or publication of private life claim.")

Instead, courts have held that personal or private information includes a person's "personal credit card, financial, bank account or medical information." BPS Direct, 705 F. Supp. 3d at 340.

Plaintiffs argue that Defendant AddShoppers may be collecting other, more personal information but they fail to plead with specificity what this personal information consists of. (See Doc. No. 69 at 5 n. 3.) For example, in the Complaint, Plaintiffs allege AddShoppers "collects every type of data imaginable," but when Plaintiffs requested "a download file of their data from AddShoppers," they only information in their files were "their email address and certain Co-Op websites time stamps." (Doc. No. 1 at ¶ 52.) As a result, Plaintiffs' allegations that AddShoppers is simply omitting from their downloaded files "the vast amount of additional information" it collects on Plaintiffs is mere speculation. (See id.) Similarly, in their Supplemental Memorandum, Plaintiffs assert that the "AddShoppers profile may also include other personal information like IP addresses, phone numbers, browser characteristics, cookies, and session information." (Doc. No. 69 at 5 n. 3 (emphasis added).) But this assertion is again speculative. And allegations that AddShoppers' consumer profiles may contain personal information are "far too speculative to support standing." Barclift, 93 F.4th at 147; see also Farst v. Autozone, Inc., 700 F. Supp. 3d 222, 232 (M.D. Pa. 2023) (finding allegations of speculative future harm "not creditable as a concrete injury in fact"). Without specific, plausible allegations that Defendants disclosed their personal or private information, such as, for example, their personal credit card, financial, bank account or medical information, Plaintiffs' asserted harm does not bare a "close relationship" to the harms recognized in traditional intrusion on privacy and seclusion claims.

Accordingly, the Court will grant Defendants' Motions to Dismiss (Doc. Nos. 25, 26, 31) for lack of Article III standing under Federal Rule of Civil Procedure 12(b)(1). While a lack of

standing is a fundamental flaw to Plaintiffs' Complaint that would alone warrant dismissal,[6] alternative bases for dismissal exist under Rules 12(b)(2) and 12(b)(6).

B. The Court Lacks Personal Jurisdiction Over Defendant AddShoppers

In its Motion to Dismiss, Defendant AddShoppers asserts that the Court does not have general or specific jurisdiction over it.[7] (Doc. No. 31-1 at 11-17.) "Personal jurisdiction may be either general or specific." General Elec. Co. v. Deutz AG, 270 F.3d 144, 150 (3d Cir. 2001). A court may exercise general jurisdiction over a nonresident party when "their affiliations with the State are so 'continuous and systematic' as to render them essentially at home in the forum State." Daimler AG v. Bauman, 571 U.S. 117, 127 (2014) (citations omitted). "For a corporation, 'the place of incorporation and principal place of business' are where it is 'at home' and are, therefore, the paradigm bases for general jurisdiction." Malik v. Cabot Oil & Gas Corp., 710 F.App'x 561, 563 (3d Cir. 2017) (citing Daimler, 134 571 U.S. at 127). Additionally, a foreign corporation registered to do business in Pennsylvania consents to Pennsylvania's exercise of general personal jurisdiction over it. Mallory v. Norfolk S. Railway Co., 600 U.S. 122, 134 (2023).

Here, because Defendant AddShoppers is incorporated in Delaware and has its principal place of business in North Carolina, it is not at home in Pennsylvania. (Doc. No. 1 at ¶ 8.)

---

[6] While this case is being filed as a class action, the named plaintiffs, specifically Plaintiffs Ingrao and Pacana, must have standing for the case to proceed. See Spokeo, 578 U.S. at 338 n. 6 ("That a suit may be a class action . . . adds nothing to the question of standing, for even named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong.'")

[7] The issue of personal jurisdiction is also raised by Defendant Vivint. (See Doc. No. 26 at 4-10.) But because Vivint is registered to do business in Pennsylvania, it is subject to general jurisdiction in Pennsylvania. (See Doc. No. 1 at ¶ 10); Mallory v. Norfolk S. Railway Co., 600 U.S. 122 (2023). While Defendant Nutrisystem did not raise the issue of jurisdiction, the Court also has general jurisdiction over it because it is incorporated and has its principal place of business in Pennsylvania. (Id. at ¶ 9.)

Moreover, there are no allegations that AddShoppers is registered to do business in Pennsylvania. Therefore, the Court will confine the inquiry to whether it exercises specific jurisdiction over AddShoppers.

The Supreme Court of the United States has articulated two tests for specific jurisdiction: (1) the Calder "effects" test or (2) the traditional "minimum contacts" test. "The Calder 'effects' test requires a plaintiff to plead facts establishing that: (1) the defendant committed an intentional tort; (2) the plaintiff felt the brunt of the harm in the forum; and (3) the defendant expressly aimed his tortious conduct at the forum." Hasson v. FullStory, Inc., 114 F.4th 181, 187 (3d Cir. 2024). The traditional test for specific jurisdiction also entails a three-step analysis. D'Jamoos ex rel. Est. of Weingeroff v. Pilatus Aircraft Ltd., 566 F.3d 94, 102 (3d Cir. 2009). First, the court must evaluate whether the defendant established minimum contacts by "deliberately 'reach[ing] out beyond' its home—by, for example, 'exploit[ing] a market' in the forum State or entering a contractual relationship centered there." Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct., 592 U.S. 351, 359 (2021) (quoting Walden v. Fiore, 571 U.S. 277, 285 (2014)). Second, the court must determine whether the litigation "arise[s] out of or relate[s] to" at least one of those contacts. Ford Motor, 592 U.S. at 352 (quoting Bristol-Myers Squibb Co. v. Super. Ct. of Cal., S. F. Cnty., 582 U.S. 255, 262 (2017)). Third, if the first two requirements are met, a court may consider whether exercising personal jurisdiction over the defendant "offend[s] traditional notions of fair play and substantial justice." Ford Motor, 592 U.S. at 358 (quoting International Shoe Co. v. Washington, 326 U.S. 310, 316-17 (1945)).

The Third Circuit Court of Appeals recently clarified that, while Calder's "effects" test is often applied "in assessing personal jurisdiction over intentional tortfeasors, . . . Calder [did not] carve out a special intentional torts exception to the traditional specific jurisdiction analysis."

Hasson, 114 F.4th at 189 (alteration in original). Accordingly, the Court will consider whether it has specific jurisdiction over Defendant AddShoppers under both the Calder "effects" test and the traditional test. See id. at 197 ("Though we agree with its application of Calder, the District Court also should have considered whether specific personal jurisdiction was proper under the traditional test as applied in Ford Motor.")

1. The Court Does Not Have Specific Jurisdiction Over Defendant AddShoppers Under the Calder "Effects" Test

Defendant AddShoppers argues that the Court does not have specific jurisdiction under the Calder "effects" test because it did not "expressly aim" its alleged conduct at Pennsylvania, as required by the third prong of the "effects" test. (Doc. No. 31-1 at 11.) To satisfy the express aiming prong, the plaintiff must do the following: (1) "show that the defendant knew that the plaintiff would suffer the brunt of the harm caused by the tortious conduct in the forum," and (2) "point to specific activity indicating that the defendant expressly aimed its tortious conduct at the forum." IMO Industries, Inc. v. Kiekert AG, 155 F.3d 254, 266 (3d Cir. 1998) (emphasis added).

Here, because Plaintiffs fail to meet the requirements to satisfy the express aiming prong, the Court does not have specific jurisdiction over Defendant AddShoppers under the "effects" test. First, Plaintiffs do not allege Defendant AddShoppers had knowledge that Plaintiffs would suffer the brunt of the harm in Pennsylvania. In this regard, the Third Circuit's opinion in Hasson v. FullStory, Inc., 114 F.4th 181 (3d Cir. 2024) is instructive here. In Hasson, a Pennsylvania resident sued a software company that produced a "Session Replay Code," which is alleged to have wiretapped and received the data collected from the plaintiff's browsing sessions. Hasson, 114 F. 4th at 195. The plaintiff argued the court had personal jurisdiction over the software company because it had "partnered with Pennsylvania companies whose websites were accessible there" and "received communications intercepted from Pennsylvanians while they were in

Pennsylvania." Id. In concluding that the plaintiff did not allege the software company had knowledge that the plaintiff would suffer the brunt of the harm in Pennsylvania, the Third Circuit held that the plaintiff must allege the defendant "knew that he—or any other user—was in Pennsylvania before [the code] was dispatched to his browser." Id. at 196 (emphasis in original). This allegation was not made in the complaint nor could it be. See id.

Moreover, the Third Circuit explained it was not persuaded by the argument that the software company "aimed its alleged wiretapping at Pennsylvania just because it knew" that its partners "conducted business in the forum or made its website accessible there." Id. The court also "rejected the argument that the 'expressly aiming' requirement is satisfied when the defendant is alleged to have engaged in wrongful conduct targeted at a plaintiff whom the defendant knows to be a resident of the forum state." Id. at 196 (internal citations omitted). "Indeed, while a defendant's 'knowledge that the plaintiff is located in the forum is necessary to the application of Calder,' that 'alone is insufficient to satisfy the targeting prong of the effects test.'" Id.

Here, Plaintiffs proffer a similar argument to the plaintiff in Hasson, contending that the knowledge requirement is satisfied because "AddShoppers knew harm would occur in Pennsylvania because it placed wiretaps on many Pennsylvania businesses' websites" and thus "knew that a significant number of Pennsylvanians would visit its partner websites because they form a significant portion of both companies' target market." (Doc. No. 39 at 15.) But, like the plaintiff in Hasson, Plaintiffs fail to allege Defendant AddShoppers knew that Plaintiffs were in Pennsylvania before the tracking code was dispatched to their browsers. Instead, again like the plaintiff in Hasson, Plaintiffs argue that AddShoppers aimed its alleged wiretapping at Pennsylvania because it knew its partners conducted business in Pennsylvania. But, like the Third Circuit in Hasson, this Court is not persuaded that this knowledge is sufficient to satisfy the

"expressly aiming" requirement. Further, Plaintiffs allegations that the knowledge requirement is satisfied because AddShoppers knew "a significant number of Pennsylvanians" would visit its partners' websites fails because mere knowledge that a person is a resident of a state is insufficient. As the Hasson court explained, "while a defendant's 'knowledge that the plaintiff is located in the forum is necessary to the application of Calder,' that 'alone is insufficient to satisfy the targeting prong of the effects test.'" Hasson, 114 F. 4th at 196.

Second, Plaintiffs also fail to point to specific activity indicating that Defendant AddShoppers expressly aimed its tortious conduct at Pennsylvania. Hasson is again instructive here. In Hasson, the Third Circuit also concluded that the plaintiff had not pointed to specific activity indicating the software company had expressly aimed its Session Replay Code at Pennsylvania. Hasson, 114 F. 4th at 195. In coming to this conclusion, the Third Circuit explained that a software company does not expressly target Pennsylvania "simply by providing code for" a website that is accessible there. Id. at 195-96.

Here, Plaintiffs argue that Defendant AddShoppers expressly aimed its conduct at Pennsylvania by orchestrating "a scheme with thousands of retailers," many of which are alleged to be Pennsylvania companies, "to (1) intercept and collect information that consumers shared with those retailers; and (2) use that collection of information to send unwanted emails to the devices of those consumers." (Doc. No. 39 at 13.) But AddShoppers is alleged to accomplish this "scheme" by installing tracking cookies on the consumers' browsers which makes Plaintiffs' argument analogous to that made in Hasson: that by simply providing code for websites that are accessible in Pennsylvania, AddShoppers targeted its conduct at Pennsylvania. And as the Third Circuit explained in Hasson, a software company does not expressly target Pennsylvania "simply by providing code for" a website that is accessible there. Hasson, 114 F. 4th at 195-96. Moreover,

unlike the plaintiff in Hasson who was in Pennsylvania when the software company allegedly wiretapped him, Plaintiffs here fail to specify their location where AddShoppers allegedly wiretapped them.

Plaintiffs attempt to distinguish this case from Hasson by arguing that the software company in Hasson did not have direct contact with the plaintiff while Defendant AddShoppers did directly interact with Plaintiffs when it emailed them. (Id. at 14.) But Plaintiffs fail to allege "they were physically located in Pennsylvania when their internet activity was supposedly tracked, or when they allegedly received emails from AddShoppers." (Doc. No. 56 at 4.) Without alleging Plaintiffs were in Pennsylvania when they received the emails from AddShoppers, whether AddShoppers directly interacted with Plaintiffs is immaterial to Plaintiffs' express aiming argument. And even if Plaintiffs could allege they were in Pennsylvania when they received emails from AddShoppers, this alone is not sufficient to conclude AddShoppers expressly aimed its conduct at Pennsylvania. See Britax Child Safety, Inc. v. Nuna Int'l B.V., 321 F. Supp. 3d 546, 557 (E.D. Pa. 2018) (concluding the defendant sending "promotional emails through its website to residents of this District" is not enough "to confer personal jurisdiction"). Accordingly, the Court does not have specific jurisdiction over Defendant AddShoppers under Calder's "effects" test and will proceed to assessing whether it has specific jurisdiction under the traditional test.[8]

[8] Because the Court has found Plaintiffs failed to allege Defendant AddShoppers expressly aimed its conduct at Pennsylvania, as required by the third prong in Calder's three-prong "effects" test, there is no need to assess whether Plaintiffs alleged AddShoppers committed an intentional tort or whether Plaintiffs felt the brunt of the harm in Pennsylvania, the other two prongs of the Calder "effects" test.

2. The Court Does Not Have Specific Jurisdiction Over Defendant AddShoppers Under the Traditional Test

Defendant AddShoppers next argues that the Court does not have specific jurisdiction under the traditional test because Plaintiffs cannot meet the three steps required to establish traditional specific jurisdiction. (Doc. No. 68 at 2.) To reiterate, specific jurisdiction under the traditional test requires the plaintiff to establish the following: (1) the defendant established minimum contacts with the forum state; (2) the litigation "arise[s] out of or relate[s] to" at least one of those contacts; and (3) if the first two requirements are met, exercising personal jurisdiction over the defendant does not "offend traditional notions of fair play and substantial justice." Ford Motor, 592 U.S. at 352, 358-59.

Here, the first prong is dispositive. Defendant AddShoppers did not establish minimum contacts with Pennsylvania. The minimum contacts requirement "has been defined as 'some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws.'" Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, 451 (3d Cir. 2003). In the context of session replay code, courts have held that a plaintiff must prove the defendant "purposefully deployed [Session Replay Code] to intentionally target users" in the forum state or that the defendant "knew it was targeting" the plaintiff in the forum state "at the time of the alleged wiretapping." Hasson, 114 F.4th at 191 (quoting Rosenthal v. Bloomingdales.com, LLC, 101 F.4th 90 (1st Cir. 2024) in which the First Circuit found it had no specific jurisdiction under the traditional test) (alterations in original; emphasis added).

Plaintiffs also argue that Defendant AddShoppers purposefully availed itself of the laws and benefits of doing business in Pennsylvania by "enter[ing] into agreements with numerous Pennsylvania companies . . . to install its code on their websites" and "send[ing] thousands (if not

millions) of targeted emails to Pennsylvania to exploit the Commonwealth's retail market." (Doc. No. 1 at ¶ 13; Doc. No. 69 at 2 (internal quotations omitted).) But alleging AddShoppers entered into agreements with numerous Pennsylvania companies is not sufficient to justify the exercise of jurisdiction over AddShoppers. See Mellon Bank (East) v. DiVeronica Bros., Inc., 983 F.2d 551, 557 (3d Cir. 1993) ("Contracting with a resident of the forum state does not alone justify the exercise of personal jurisdiction over a non-resident defendant.") Moreover, alleging AddShoppers sends "thousands (if not millions) of targeted emails to Pennsylvania" is similarly not enough because it does not demonstrate that AddShoppers knew the email recipients were in Pennsylvania when it sent these emails. In fact, Plaintiffs do not even allege that they were in Pennsylvania when they received AddShoppers' emails. The Complaint only specifies that Plaintiff Pacana is a resident of Pennsylvania but fails to allege Plaintiff Pacana was in Pennsylvania when any of the conduct at issue took place.[9] (See Doc. No. 1 at ¶ 7.)

Accordingly, the Court does not have specific jurisdiction over Defendant AddShoppers under the traditional test and will grant its Motion to Dismiss (Doc. No. 31) for lack of personal jurisdiction under Federal Rule of Civil Procedure 12(b)(2). As mentioned above, while the Court's above findings that Plaintiffs lack standing under Rule 12(b)(1) and lack personal jurisdiction under Rule 12(b)(2) would alone warrant dismissal of Plaintiffs' claims, the Court has an alternative basis for dismissal for Plaintiffs' failure to state a claim under Rule 12(b)(6).

[9] Because the Court has found that Plaintiffs failed to allege Defendant AddShoppers purposefully availed itself of the laws and benefits of doing business in Pennsylvania, as required by the minimum contacts prong of the traditional test for specific jurisdiction, there is no need to assess whether the litigation arises out of or relates to one of AddShoppers' contacts with Pennsylvania nor if the Court's exercise of personal jurisdiction over AddShoppers offends traditional notions of fair play and substantial justice, as required in the second and third prongs of the traditional test.

C. Plaintiffs Failed to State a Claim Under WESCA, CIPA and the CDAFA

Defendants argue that Plaintiffs claims under the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA") (Counts I, II, and III), the California Invasion of Privacy Act ("CIPA") (Count IV) and the California Computer Access and Data Fraud Act ("CDAFA") (Count V) should be dismissed for failure to state a claim under Rule 12(b)(6). (See generally Doc. Nos. 25, 26, 31.) The Court will discuss the claims made in the Complaint under WESCA, CIPA and the CDAFA in turn.

1. Plaintiffs Fail to State a Claim Under the Pennsylvania Wiretapping and Electronic Surveillance Control Act

Plaintiff Ingrao brings a WESCA claim against Defendant Nutrisystem (Count I) while Plaintiff Pacana brings WESCA claims against both Defendant AddShoppers (Count II) and Defendant Vivint (Count III). (Doc. No. 1 at ¶¶ 81-125.) WESCA is Pennsylvania's state law equivalent to the Federal Wiretap Act. See Popa v. Harriet Carter Gifts, Inc., 52 F.4th 121, 125 (3d Cir. 2022) (explaining WESCA "operates in conjunction with and as a supplement to the Federal Wiretap Act, 18 U.S.C. § 2510, which provides uniform minimum protections for wire, electronic, or oral communications"). "The WESCA offers a private civil cause of action to '[a]ny person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of [that statute]' against 'any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication.'" Id. at 125; see also 18 PA. CONS. STAT. § 5703.[10]

[10] Specifically, WESCA prohibits a person from doing the following:

> (1) intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept any wire, electronic or oral communication;
>
> (2) intentionally disclos[ing] or endeavor[ing] to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived

In other words, WESCA "prohibits intercepting communications." Id. The Court will assess Plaintiff Ingrao's WESCA claim separately from Plaintiff Pacana's WESCA claims.

a. Plaintiff Ingrao's Pennsylvania Wiretapping and Electronic Surveillance Control Act Claim Against Defendant Nutrisystem

Defendant Nutrisystem argues Plaintiff Ingrao's WESCA claim should be dismissed because she did not allege she was in Pennsylvania when Nutrisystem purportedly intercepted her communication. (Doc. No. 25 at 6-7.) The Third Circuit has limited liability under WESCA only to those communications intercepted at servers located within Pennsylvania's borders. Popa, 52 F.4th at 131. Electronic communications are intercepted at the point where they are routed to the interceptor's servers, meaning at the plaintiff's server rather than the defendant's server. Id. at 132. For example, in Popa, a Pennsylvania resident brought a WESCA claim against a Virginia software company, alleging the company had intercepted her communications. Id. at 125. In determining where the interception took place, the Third Circuit held that the defendant software company had intercepted the plaintiff's communications at the plaintiff's server, rather than at the company's Virginia servers, because that is where the defendant's software rerouted the plaintiff's communications. Id. at 131.

Here, Plaintiff Ingrao is a resident of California who claims her visit to Nutrisystem's website was tracked by Nutrisystem's browser cookies. (See Doc. No. 1 at ¶¶ 55, 57.) While

---

> therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or
>
> (3) intentionally us[ing] or endeavor[ing] to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic or oral communication.

18 PA. CONS. STAT. § 5703.

Defendant Nutrisystem is a Pennsylvania corporation whose servers are presumably located in Pennsylvania, the Third Circuit in Popa made clear that the point of interception is at the plaintiff's server rather than the interceptor's server. Based on this notion, if Defendant Nutrisystem intercepted Plaintiff Ingrao's communications, this interception occurred at Plaintiff Ingrao's server where she visited Nutrisystem's website. But Plaintiff Ingrao fails to allege where she accessed Defendant Nutrisystem's website, although it most likely was located in California. Moreover, the Complaint is devoid of any allegations that Plaintiff Ingrao was ever present in Pennsylvania, much less that she visited Nutrisystem's website while in Pennsylvania. (See generally Doc. No. 1.) Because there are no allegations that Nutrisystem's alleged interception occurred in Pennsylvania, Plaintiff Ingrao has failed to state a claim against Defendant Nutrisystem under WESCA. Accordingly, Defendant Nutrisystem's Motion to Dismiss Plaintiff Ingrao's WESCA claim in Count I will be granted.

b. Plaintiff Pacana's Pennsylvania Wiretapping and Electronic Surveillance Control Act Claims Against Defendant AddShoppers and Defendant Vivint

Defendants AddShoppers and Vivint argue that Plaintiff Pacana's WESCA claims should be dismissed because she fails to allege they intercepted any "contents" of her electronic communications.[11] (Doc. No. 26 at 16-18; Doc. No. 31-1 at 14-15.) As mentioned above, WESCA "prohibits intercepting communications." Popa, 52 F.4th at 125. WESCA defines "intercept" as

[11] Like Defendant Nutrisystem, Defendants AddShoppers and Vivint also argue that Plaintiff Pacana's WESCA claims should be dismissed because she fails to allege her communications were intercepted in Pennsylvania. (See Doc. No. 26 at 23; Doc. No. 31-1 at 19.) In this regard, the Complaint contains no allegations specifying where Plaintiff Pacana was located when Defendants AddShoppers and Vivint allegedly intercepted her communications. (See generally Doc. No. 1.) But Plaintiff Pacana, unlike Plaintiff Ingrao, is a resident of Pennsylvania. (Id. at ¶ 7.) For this reason, the Court is unwilling to draw an adverse inference regarding Plaintiff Pacana's location at the time of the alleged interception, and will instead focus its assessment on AddShoppers' and Vivint's other arguments.

the "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 PA. CONS. STAT. § 5702 (emphasis added). Moreover, WESCA defines "contents" as "any information concerning the substance, purport, or meaning of that communication." Id. "Because the relevant provisions and statutory definitions (e.g., "intercept" and "contents") from [WESCA] are identical to those in the [Federal Wiretap Act, 18 U.S.C. § 5725(a)], the Court can look to decisions applying those provisions and definitions for guidance." Cook, 689 F. Supp. 3d at 68 n. 6.

Courts have interpreted "contents" as referring "to the intended message conveyed by the communication, [which] does not include record information regarding the characteristics of the message that is generated in the course of the communication." In re Zynga Priv. Litig., 750 F.3d 1098, 1106 (9th Cir. 2014) (interpreting the Federal Wiretap Act). "Thus, determining whether a plaintiff has adequately pled a violation of the statute often comes down to deciding whether the acquired information can best be characterized as either 'record information' or 'the message conveyed by the communication.'" Cook, 689 F. Supp. 3d at 68-69. In Cook, the court considered whether the defendant's session replay code intercepted contents of the plaintiff's communications when the plaintiff alleged it intercepted her "mouse movements and clicks, keystrokes, and URLs of web pages visited." Id. at 70. The court held that "[n]one of this information constitutes 'contents' of 'communications.'" Id.

Here, Defendant AddShoppers argues Pacana's WESCA claim against it centers around the allegation that "AddShoppers installs [] tracking technology on partner websites, which secretly intercepts visitors' electronic communications with the websites in real time." (Doc. No. 31-1 at 20.) "Nowhere, however, does Pacana describe the contents of her [] electronic communications that were allegedly intercepted." (Id.) And Defendant Vivint asserts "Pacana did not identify what

information, if any, Vivint allegedly collected from her visit to its website." (Doc. No. 26 at 17-18.) In response, Plaintiff Pacana makes vague arguments about captured URLs being "potentially content." (Doc. No. 39 at 18.) But "[l]ocation identifiers, like URLs, 'have classically been associated with non-content means of establishing communication." Cook, 689 F. Supp. 3d at 71 (quoting In re Google Inc. Cookie Placement Cons. Priv. Litig., 806 F.3d 125, 136 (3d Cir. 2015) [hereinafter Google Cookie]). "Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging . . . that search term to a third party could amount to disclosure of the contents of a communication." In re Zynga, 750 F.3d at 1108-09. However, Pacana only alleges she visited the websites of retailers partnered with AddShoppers, including a retailer called Lamin-x and Defendant Vivint. (Doc. No. 1 at ¶¶ 61, 66.) She does not allege she searched for any specific information and even admits she "never provided any personal information (including her email) to Vivint" or Lamin-x. (Id.)

Pacana does specify that, after requesting her data from AddShoppers, she discovered the data contained "the exact dates and times she visited other websites that (unbeknownst to her) were part of AddShoppers network." (Id. at ¶ 66.) For example, this data contained a report on the date and time Plaintiff Pacana visited Defendant Vivint's website. (Id.) But these dates and times are not substantive information—instead, they are "the cyber analog to record information [AddShoppers and Vivint] could have obtained through a security camera at a brick-and-mortar store." Cook, 689 F. Supp. 3d at 70.

In a final attempt to allege it captured the "contents" of her electronic communications, Pacana argues AddShoppers tracking "code is designed to intercept a person's electronic conversation with a website including the precise webpages they visit." (Doc. No. 69 at 13 (emphasis added).) But "it is not enough for [Pacana] to allege the potential capabilities of the

[tracking code]. Rather, she needed to allege that [AddShoppers and Vivint], in fact, harnessed the capabilities she describes, and it had the result of capturing the contents of specific communications." Cook, 689 F. Supp. 3d at 69. But Pacana did not make such allegations.

Accordingly, Defendant AddShoppers and Defendant Vivint's Motions to Dismiss Plaintiff Pacana's WESCA claims in Counts II and III will be granted.

2. Plaintiff Ingrao Fails to State a Claim Under the California Invasion of Privacy Act

In Count IV, Plaintiff Ingrao brings a CIPA claim against Defendant Nutrisystem. (Doc. No. 1 at ¶¶ 126-34.) CIPA, like WESCA, "broadly prohibits the interception of wire communications and disclosure of the contents of such intercepted communications." Google Cookie, 806 F.3d at 152; see also CAL. PENAL CODE § 631(a).[12] Also like WESCA, courts analyze

[12] Specifically, CIPA provides as follows:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both a fine and imprisonment in the county jail or pursuant to subdivision (h) of Section 1170. If the person has previously been convicted of a violation of this section or Section 632, 632.5, 632.6, 632.7, or 636, the offense is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both that fine and imprisonment.

CIPA claims under the same standards as the Federal Wiretap Act. See Google Cookie, 806 F.3d at 152 (concluding the plaintiff's CIPA claim failed for the same reasons its Federal Wiretap Act claim failed); In re Nickelodeon Cons. Priv. Litig., 827 F.3d 262, 276 (3d Cir. 2016) (same). In that regard, CIPA's use of "contents" has the same meaning as "contents" under WESCA: "'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." See In re Zynga, 750 F.3d at 1106 (interpreting the Federal Wiretap Act); see also Cole v. Quest Diagnostics, Inc., No. X, 2024 WL 3272789, at *4 (D.N.J. July 2, 2024) ("Federal courts have routinely analogized the definition of 'content' under CIPA with the definition under the Wiretap Act.").

Here, because CIPA and WESCA have the same meaning for their respective use of the word "contents," Plaintiff Ingrao's CIPA claim fails for the same reasons Plaintiff Pacana's WESCA claims failed. Namely, they each cannot allege that "contents" of their communications were intercepted by Defendants. Like Plaintiff Pacana, Plaintiff Ingrao vaguely alleges that AddShoppers' tracking cookies "tracked [her] precise webpage visit" to Defendant Nutrisystem's website. (Doc. No. 1 at ¶ 56.) However, unlike Plaintiff Pacana, Plaintiff Ingrao is unable to even allege Nutrisystem had captured "the exact dates and times" she visited its website. Instead, she describes requesting "her data from AddShoppers" and discovering "she had been tracked by many companies for several years." (Id. at ¶ 59.) But she does not allege any content captured by Defendant Nutrisystem or any of the other "many companies."

CAL. PENAL CODE § 631(a).

Moreover, while Plaintiff Ingrao received an email from "Nutrisystem via SafeOpt" after her visit to Nutrisystem's website, she admits to never having "provided any personal information to that company." (Id. at ¶ 55.) But based on Ingrao having received an email from "Nutrisystem via SafeOpt" the same evening she visited the Nutrisystem website, the Court will construe this in the light most favorable to Plaintiff Ingrao and infer that Defendant Nutrisystem at least captured her visit to its website. However, as above, that Plaintiff Ingrao visited Defendant Nutrisystem's website is not substantive information—instead, it is "the cyber analog to record information [Nutrisystem] could have obtained through a security camera at a brick-and-mortar store." Cook, 689 F. Supp. 3d at 70. As such, Plaintiff Ingrao did not sufficiently allege that Nutrisystem captured "contents" of her electronic communications and Defendant Nutrisystem's Motion to Dismiss Ingrao's CIPA claim in Counts IV will be granted.

3. Plaintiff Ingrao Fails to State a Claim Under the California Computer Access and Data Fraud Act

Finally, in Count V, Plaintiff Ingrao brings a claim under the CDAFA against Defendant AddShoppers and Defendant Nutrisystem. (See Doc. No. 1 at ¶¶ 135-48.) The CDAFA aims to protect "individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." CAL. PENAL CODE § 502(a). It is essentially "an anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purpose." Custom Packaging Supply, Inc. v. Phillips, No. 2:15-CV-04584, 2015 WL 8334793, at *3 (C.D. Cal. Dec. 7, 2015). While the CDAFA is a criminal statute, it also provides for civil remedies. See CAL. PENAL CODE § 502(e). But a plaintiff's ability to bring a private suit under Section 502 hinges on whether the plaintiff suffered "damages or loss by reason of a violation." See Google Cookie, 806

F.3d at 152 (quoting CAL. PENAL CODE § 502(e)(1)) ("[A] suit [under Section 502] may only be brought by one who has 'suffere[d] damage or loss by reason of a violation'").[13]

The majority of courts to consider the issue have held that "damage or loss" under the CDAFA "contemplates some damage to the computer system, network, program, or data contained on that computer, as opposed to data generated by a plaintiff while engaging with a defendant's website." See Heiting v. Taro Pharm. USA, Inc., 709 F. Supp. 3d 1007, 1021 (C.D. Cal. 2023) (emphasis added) (rejecting the argument that the plaintiff's loss of data, including "IP address information and other identifying information," is "damage" or "loss" under the CDAFA); see also Google Cookie, 806 F.3d at 148-49 (rejecting the plaintiffs' argument that they suffered loss under the CDAFA through the defendants' "capturing and making economic use of [the plaintiffs' personally identifiable information]" thus "depriving the plaintiffs of their own ability to sell their internet usage information"); Cottle v. Plaid Inc., 536 F. Supp. 3d 461, 488 (N.D. Cal. 2021) (holding damage or loss under the CDAFA did not include "loss of the right to control [the plaintiffs'] own data, the loss of the value of their data, and the loss of the right to protection of the data"); Doe v. Meta Platforms, Inc., 690 F. Supp. 3d 1064, 1081-83 (N.D. Cal. 2023) (holding the plaintiffs' allegations that their protected information was diminished in value did not qualify as damage or loss under the CDAFA); Pratt v. Higgins, No. 22-cv-04228, 2023 WL 4564551, at

[13] Section 502(e)(1) provides in relevant part:

> [T]he owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief.

CAL. PENAL CODE § 502(e)(1) (emphasis added). Here, Defendants AddShoppers and Nutrisystem are alleged to have violated various subsections of Section 502(c). (See Doc. No. 1 at ¶¶ 137, 140-42, 144.)

*9 (N.D. Cal. July 17, 2023) (finding the defendant's access to the plaintiff's communications, notes and medical information did not create the type of loss contemplated by the CDAFA's private cause of action).

Here, because Plaintiff Ingrao fails to allege she suffered the requisite "damage or loss" from Defendants AddShoppers' and Nutrisystem's alleged CDAFA violation, she cannot seek civil relief under Section 502. Plaintiff Ingrao argues she suffered a loss through the deprivation her "of the value of [her] personally identifiable data." (Doc. No. 1 at ¶ 140; Doc. No. 39 at 25.) But this argument is identical to the loss argument rejected by a majority of courts, as listed supra. Because Ingrao only alleges the loss of data generated while she engaged with Defendant AddShoppers' partner websites, including Defendant Nutrisystem's website, rather than damage to her computer system, network, program, or data contained on her computer as required to recover under the CDAFA, she fails to state a civil claim under the CDAFA. Accordingly, Defendant AddShoppers' and Defendant Nutrisystem's Motions to Dismiss Plaintiff Ingrao's CDAFA claim in Count V will be granted.

V. CONCLUSION

For the foregoing reasons, Defendants' Motions to Dismiss the Complaint (Doc. Nos. 25, 26, 31) will be granted. An appropriate Order follows.